Comment for Proceeding 12-52, Proceeding 08-146, Proceeding 07-287, Proceeding 11-82, Proceeding 11-60, Proceeding 06-119 – "Certain Wireless Service Interruptions" / "CMS Licensees" / "In the Matter of the Commercial Mobile Alert System" / "Proposed extension of Prat 4 of the Commission's Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers" / "Reliability and continuity of Communications Networks, Including Broadband technologies' effects on Broadband Communications Networks of Damage or Failure of Network Equipment or severe overload" / "FCC seeks Comment on Recommendation of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks"

In the Notice for Proceeding 12-52, it is stated that "the Federal Communications Commission's (FCC or Commission) Public Safety and Homeland Security Bureau (PSHSB) and Wireless Telecommunications Bureau (WTB) seek comment on concerns and issues related to intentional interruptions of Commercial Mobile Radio Service (CMRS or "wireless service") by government authorities for the purpose of ensuring public safety."
This comment will address each of the questions posed in the Notice for the proceeding (12-52), and where possible will provide examples of situations or circumstances in which the answers would apply, or have applied. The comments, in keeping with the focus of the proceeding as described by the Notice, will be oriented to "interruptions of wireless service that are conducted or initiated by government authorities."
A portion of this comment also briefly address issues in response to Proceedings 08-146 and 07-287. In these proceedings, the issues relating to the Commercial Mobile Alert System have direct bearing upon concerns which are raised here within Proceeding 12-52. Finally, in addition, this comment is also intended to express support for the Federal Communication Commission's Report and Order of February 15, 2012, in connection with PS Docket No. 11-82 that mandatory outage reporting will be required of Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers. (With the increasing use of such VoIP services on our cell phones as an example, as customers we have a need to know what is happening very quickly and any providers engaging in cellular "interruptions" must be held accountable under the Communications Act without the opportunity of forbearance, in my view.) However, this comment, and the answers to the following questions, are filed in all proceedings referenced above. Comments are sought from interested individuals and organizations (governmental and non-governmental alike) on the substance of this comment.

1. Past practices and precedents. As noted above, last summer a public agency cited public safety concerns as a reason for temporarily interrupting wireless service on certain portions of a mass transit system. What are examples of previous intentional interruptions of wireless service for public safety reasons, and what policies or rationales have public agencies developed that support or provide guidance on such interruptions?
a. Under what circumstances have public agencies in the United States considered or effectuated interruptions of wireless service for public safety reasons?

The notable cases that answer this question are:
A. People v. Brophy, 49 Cal. App. 2d 15 - Cal: Court of Appeal 1942
1. It is this case that provides the best guidance, in particular in the context of California and with respect to the most recent intentional interruption of which I am aware (on August 11, 2011, in California, which occurred as a result of SFBART action).
B. The SFBART (or BART) intentional interruption (service modification on August 11, 2011).
1. To date, there is no sound legal rationale that would support a public agency action to either interrupt completely or in part (modify, for example, by throttling or perhaps by shutting off) a cellular network and / or a wireless internet network.
2. BART has developed a policy, which has been adopted by its Board, but this policy does not provide guidance for the Board, its employees, or agents, to seek an order from the Commission, a state commission of appropriate jurisdiction, or a court of law with appropriate jurisdiction prior to any modification or discontinuance sought, and thus the policy is entirely inadequate. (Nor does it make any reference to the FCC's policies, website, or protocol on discontinuance of service.)
3. More than anything, this BART policy reveals an assumption of the BART Board that it can operate outside of the realm of the law.

b. What are relevant examples of foreign governments considering or effectuating interruptions of wireless service for public safety reasons? What laws or policies do foreign states have regarding interruption of wireless service for purposes of protecting public safety?

Immediately what comes to mind is Egypt, but also China, North Korea, and more recently Iran. There are actually various other cases as well. However, in my comment, I do not seek to cite the laws of various foreign states because not only in my observation is the interruption of wireless service merely for public safety reasons contrary to U.S. law, it is offensive to basic principles of human dignity and freedom, and in my personal observations, the applications of the law in various countries such as those I have mentioned above have not served the people of those countries, and we are perilously close to losing the vestiges of what remains of what is supposed to be defended (in the public interest) by the U.S. legal system, here, and are fast becoming not so different,

really, from the aforementioned countries with respect to how people's rights are contemplated and defended by agencies and courts. So I would rather not comment on laws or policies of foreign states. Let us focus instead on how to apply our laws here and defend the rights of people in the United States.

c. What are examples of wireless networks actually being used to put the public's safety at risk? Could interruption of wireless service have mitigated these harms? How would such interruptions have mitigated these harms?

If we assume that interruption of wireless service can mitigate a harm that could occur from a malicious use of a wireless network, then we can also assume that interruption of any network, regardless of whether or not it is wireless, could mitigate a harm that could occur from a malicious and potentially harmful use of a network. In other words, the idea here seems to be, give any kind of government within the U.S. the power to interrupt networks – without any real oversight or significant bar for approval from the courts or the FCC -- and we'll all be safer. That's the furthest from the truth. The gravest harm that could occur, in fact, is the idea that denial of access to what should be a public system will mitigate a public risk. We need only step back and look at Sept 11, and observe what happened when in the wake of the attack, people communicated about the evolving emergency using early cell phones and in-plane credit-card phones – and when a cell tower went down, interrupting service, people were able to continue to communicate using Blackberries. (You can look at the 9/11 Commission Report for some details on this.) The 9/11 Commission staff stated, regarding the individuals on United Flight 93 (and others), "Their actions saved the lives of countless others, and may have saved either the U.S. Capitol or the White House from destruction." The Emergency Alert System was never activated – media response was sufficient such that it never needed to be, according to most accounts. Think about that very carefully. Today's real media is social media, with a majority of people accessing information or disseminating information via this information via their cell phones. Again, think very carefully about the implications of this.

In a very serious emergency that is similar in type to what occurred on 9/11, it is entirely reasonable to state that the CMAS now being developed and implemented would also never need to be activated. Ensuring that networks remain on and that people are able to remain able to communicate across them would be of primary importance to public safety.

In addition, a recent report reveals that:

88% of American adults own a cell, 57% a laptop, 19% an e-reader, 19% a tablet; and 63% go wireless online with at least one of these devices: http://bit.ly/I8Qi4L (from a new Pew Report on Internet access, dated April 13, 2012 by Kathryn Zickuhr and Aaron Smith of the Pew Internet & American Life Project). The summary of this report also states "young adults, minorities, those with no college experience, and those with lower household income levels are more likely than other groups to say that their phone is their maine source of internet access." (The full report is available at http://pewinternet.org/Reports/2012/Digital-differences.aspx) In other words, a majority of American adults in any area to be targeted for a cellular and / or wireless internet shutdown by the government would be significantly and negatively impacted, and their safety would be put at risk.

I also encourage you to review a recent Open Net Initiative report dated April 3, 2012 at
http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance

d. What existing policies do public agencies in the United States have for determining whether a service interruption is proper? What existing policies or agreements do public agencies in the United States have for effectuating an interruption of wireless service?

Absent a survey of U.S. public agencies, which would probably be nonresponsive to these questions, please refer to section B.2 of my answer to question 1, above.

2. Bases for interrupting wireless service. Under what circumstances, if any, is it appropriate for a public agency to interrupt wireless service? How effective is an interruption likely to be in achieving the purpose of the interruption?
a. What types of government authorities are most likely to seek intentionally to interrupt wireless service?

Because of the nature of the sort of events described in my answer to 2(b) below) and the kind of government authorities that would actually have the ability or capacity to (potentially) detect and / or prevent such events from actually happening, I suppose that the DHS, and / or FBI would likely be government authorities that would be most likely to seek to intentionally interrupt wireless service. However, this is a bit of a tough question to answer, because as was seen on August 11, 2011, on the basis of fear and unwarranted speculation, and without any real demonstrable legal grounds and with no real public safety grounds that could be demonstrated in any real context from my point of view, SFBART, a special district created by the State of California (not a Federal

Agency!) went ahead and interrupted wireless service, intentionally. So, I think that if the Federal Communications Commission were to rule in a way that would make it easy for local governments to shut down CMRS, you'd probably see a rash of cases in different spots in the U.S. where quickly local governments would abuse this power, and fairly rapidly. Federal agencies are probably unlikely to do it unless there is some dire, compelling national defense related need – at least, based on what has been seen so far, a Federal action to shut off cellular service for some broad sector of the population hasn't been seen, that I'm personally aware of. However, I wouldn't recommend making it easier for Federal agencies either. If you lighten the regulatory burden, some Federal agency is going to eventually come along and abuse it.

Example of a City: Chicago seeking ability to shut down service in response to the upcoming May NATO summit protests. See this March 6, 2012 story: http://news.medill.northwestern.edu/chicago/news.aspx?id=202648

b. In what kinds of situations would a government authority potentially seek intentionally to interrupt wireless service? How frequently do these situations arise? For how long would service be interrupted in these situations? How rapidly after the threat to public safety has passed can service be restored?

I think it's obvious where a government authority will actually be seeking intentionally to do this. If it happens again in the near future it will likely be in response to a protest, but the claim will be made that it is for reasons of "public safety," like, 'our train service might be impeded' or 'we have indicators of unsafe action.' Let's dismiss this ridiculous argument now and get to real public safety arguments.

Let us suppose for a moment that you were to detect a nuclear missile honing in on active cellular signals, or you detected a Stuxnet type virus apparently propagating through a local wireless network that was about to rage through critical infrastructure, disrupting machinery that is keeping various cities' energy sources stable and free from shutdowns. In such situations, I can imagine that (in keeping with the focus of this proceeding as described by the Notice for proceeding 12-52, this comment being oriented to "interruptions of wireless service that are conducted or initiated by government authorities") a **government authority** would want to rapidly respond to such a threat, and may, as part of its response, target a portion of a network for shutdown. This question asks, however, "is it appropriate" to do so? The answer is elusive, even though for some it may seem obvious on its face, because in order to be able to deal with such situations, a government authority will not be able to contemplate every possible situation. One could get very creative and list hundreds of horror scenarios and still not begin to fill the list of an infinity in which anything, really, could happen. Thus, a government authority will at some point want a **blanket approval** to interrupt wireless service in order to address any potential public safety threat.
Such an approval is inappropriate. What is appropriate is to operate within the law. If the law does not provide efficient or rapid means for authorizing a government authority to address potentially massively destructive events then there must be a way for the courts or the FCC to be contacted rapidly (and for them to respond rapidly) in the event of potentially highly destructive situations so that a government authority can seek approval expeditiously – **but still in a manner consistent with the Communications Act, and never in a manner which allows governments to act alone or to react by doing "self-help." Furthermore, if the FCC ultimately rules that the Communications Act alone is insufficient by itself to provide regulatory authority to restrain a governmental actor from shutting off cellular and / or wireless internet service, it should rely upon other definitions provided in this comment (below), and require by ruling that governmental actors go to a court of law with appropriate jurisdiction to seek any approval for discontinuance or modification of service of any kind and any duration - in all cases prior to any discontinuance or modification (and / or what has also been referred to as "interruption," "shutoff," and similar terms).**

c. Under what circumstances would an interruption of wireless service likely be effective in protecting public safety? Under what circumstances might interrupting wireless service be ineffective?

There are probably no circumstances in which an interruption of wireless service would likely be effective in protecting public safety. In total nightmare or hell scenarios, it's likely that large numbers of people that would be impacted would have only moments until the scenario took effect and either claimed massive numbers of lives or devastated critical infrastructure, or both. You may as well leave the network on and let people help you by using it to communicate to the extent that they can.
The people are your best resource.

3. Risks in interrupting wireless service. What are the risks of an interruption of wireless service? What factors affect those risks?

a. What public safety risks arise from intentionally interrupting wireless service? How are the activities of first responders and other emergency personnel and government authorities affected by an intentional interruption of wireless service? How are the activities of consumers affected by an intentional interruption of wireless service?

Well, large numbers of people will be unable to communicate. Incidents and accidents will be unable to be reported in a timely fashion. This will impact, for example, the ability of ambulances to respond to people in critical need. It will also have an economic impact on people who rely upon cellular networks for communication routinely in order either to find their way from one place to another (this occurs a lot) and will likely disrupt the ability of people who are trying to connect with family and friends to connect for transport through or out of an urban area. This could also be a public safety issue as some of these people could get lost. In fact, a recent study revealed that numbers ranging from 1/5th to 1/3rd (depending on the locale) of 3rd graders are using cell phones. This is a growing means for young people to communicate both with parents and with each other. This gives you a little bit of an insight into who is using cell phones and just how prevalent they are in society. Indeed, age of the users of cell phones and / or wireless internet services is a factor in the risks inherent in any potential interruption of wireless service.

b. What are the potential economic consequences of intentionally interrupting wireless service?

Well, for example, we have seen that people will boycott, repeatedly protest, and conduct cyberattacks on public agencies that perform interruptions of telephone and / or wireless service (after service is interrupted). Obviously, these kinds of things have economic consequences. Other economic consequences are that financial transactions are disrupted or kept from happening which would ordinarily occur (or for which service would ordinarily be available to facilitate) across wireless networks, during the time of an interruption. Finally, it is likely that legal challenges in the courts await any public agency that attempts to do this in the future, although who (a public interest group, or affected individuals) ultimately files suit would depend on the nature of the action. All of these things have economic consequences, particularly for the public agency / governmental authority that opts to engage in intentional interruption of wireless service.

Disrupting service can also subject the party to penalties of up to $10,000 per interruption:

"Any person who willfully and knowingly does or causes or suffers to be done any act, matter, or thing, in this chapter prohibited or declared to be unlawful, or who willfully and knowingly omits or fails to do any act, matter, or thing in this chapter required to be done, or willfully and knowingly causes or suffers such omission or failure, shall, upon conviction thereof, be punished for such offense, for which no penalty (other than a forfeiture) is provided in this chapter, by a fine of not more than $10,000 or by imprisonment for a term not exceeding one year, or both; except that any person, having been once convicted of an offense punishable under this section, who is subsequently convicted of violating any provision of this chapter punishable under this section, shall be punished by a fine of not more than $10,000 or by imprisonment for a term not exceeding two years, or both." (47 U.S.C. 501)

c. How do particular circumstances affect the risks that arise from an interruption of wireless service? Are there particular kinds of locations where interruption is especially risky? Are there areas where first responders and other emergency personnel are especially dependent upon commercial wireless service to perform their duties or where consumers are particularly dependent on wireless service? How does the availability of alternative means of communication affect the risks that arise from an interruption of wireless service? Does the interruption of wireless service pose particular risks to persons with disabilities?

Cutting cell service poses the risk that emergency services may not be able to communicate with each other depending on which systems they are using and the environment in which they operate. In the Bay Area of California each law enforcement agency uses a different radio system. The only way they have of coordinating with other agencies is to call their base of operations or use wireless cell service.

"If a major earthquake were to strike one of the fault lines that runs through the Bay Area, emergency officials from across the region would largely rely on cell phones and land lines to communicate with one another."
http://blog.tcomeng.com/wp-content/uploads/2008/12/sfexaminer-getting_in_sync-02192009.pdf

Radio systems may not work on BART versus the wide coverage available on cell phone networks. For example, Paramedics carry radios that will not function while they are in BART tunnels or underground stations.

When BART cut off wireless service to their tunnels they disconnected to the back haul link, so persons close to BART, even if within range of another cell tower, still couldn't get any connectivity. People out on the street were likely impacted even though BART was only seeking to prevent people inside the immediate underground area from using their cell phones.

d. What steps could be taken to minimize the risks that arise from an interruption of wireless service? What steps could be taken to narrow the scope of a service interruption?

Don't interrupt the service.

e. What institutions or officials should be notified of an intentional interruption of wireless service? How and when should they be notified? How and when should the public be notified? Should notifications include the reason for the service interruption?

Please see my answer to 5(b) below.

f. Are there less intrusive ways of protecting public safety than interrupting wireless service? If so, what are they? Under what circumstances are these alternative means likely to be as effective as interrupting wireless service? Should government officials be required to consider alternative means before interrupting wireless service?

Yes, they should. Also, government officials, if they are doing up public safety plans, should encourage the use of mesh network applications such as the Serval Project (for phones) and / or Project Meshnet (for computers).

g. Are there situations where the risk of interrupting wireless service will always outweigh the benefits?

Yes, this is in all situations.

h. What kinds of liability issues for wireless service providers might be raised by wireless service interruptions?

N/A – No comment

4. Scope of interruption. We seek comment regarding the scope of service interruptions.

There are always several parties involved when considering wireless service. In the case of the Bay Area, it's very important to understand that although AT&T may own a BTS, they don't necessarily own the backhaul network it is connected to.

A wireless network has the following technical components:

1. the terminal device- a phone or computer modem*
2. the BTS- a base station, micro or picocell*
3. the backhaul network*
4. the routing software
5. the point of termination on the telco network

* These may involve a Distributed Antenna System in some cases.

The system does not work unless all of these are available and connected. If a BTS is present on someone's property- say attached to their building- then it is possible that they can disconnect it from the network, or from its power supply. But they do not have access to the administrative interface on that BTS or the routing software that connects it and therefore it is not possible for that property owner to implement any sort of fine-grained access control.

Now, it is possible that by intentionally disconnecting such a node that the property owner is in breach of a contract between them and the network provider.

So the parties involved in this are rather complex:

1. the network (let's say ATT)

2. the property owner on whose easement the BTS is installed

3. the backhaul network provider

4. the BTS software provider (ericsson, nokia, qualcomm)

5. the power company

6. the user, who has a contract with party 1

The actions of any of these people can cause a cessation of service but the level at which they can interact with the technology stack is different for each party.

AT&T can certainly turn down or off a BTS; it is a common activity for them to tweak a BTS in order to improve coverage or reduce interference with a neighbouring BTS. They also control the routing software, which means they have the ability to implement any level of selective service or service filtering. However, it is my understanding that if they do so with preference to any particular traffic they are in breach of their common carrier status.

Again, in the case of BART the BTS (owned by AT&T) connects to an internetwork link (owned by the BART transit district). However, it just tunnels across that network in an opaque fashion. BART physically may be able turn off components of this (even though I maintain it isn't legal to do so); they can't change the BTS' settings or filtering.
The situation in, say, a shopping mall is the same.

In order for BART to have access to change what type of service is provided, they'd have to have the ability to alter with the RF network configuration which is way outside what AT&T would ever accept. It's also not something I would trust BART staff to work on.

The performance of the radio network as a whole is based on certain principles that require advanced knowledge to understand. The reason that they are remotely controlled is that AT&T line staff are not trained to set them up. They are configured remotely from a network operations center.

So really, the question is not "can an operator do "x"" as much as "who is the operator."

In most countries, including the USA, there's a system like the Telephone Preference System. To understand why these systems are necessary, you need to know a little bit about how a phone system works. Going back to the oldest days of wired phones, you have some number of subscribers (Ns) and a switching system.

But the individual switching resources needed to make a connection from one subscriber to another are very expensive. As a consequence, the number of possible switching paths through the switch matrix is much smaller (Np). The ratio Ns:Np is called the oversubscription ratio, and is commonly on the order of 50:1. What this means is that when everyone picks up the phone at once, only 2% of them will get a dialtone; the others will get a "fast busy" or "reorder" tone.

Because this upset the government in the 1950s they implemented a priority scheme, where particular phones could be tagged as "priority one". Then when the number of free switch paths got low, they would disable phones from priority 4 downwards and a priority one phone would always get a dialtone. When phone networks became digital and packet-switched, the system got more sophisticated and the details of the system they forced on the mobile operators are actually classified, so I can't provide information about how it works.

What is definitely true is that there are systems allowing the restriction of phone origination and termination by IMEI and IMSI information; this system is also used to blacklist stolen phones. But, again, this is a system just brimming over with sensitive data, personally identifying data, and personally locating data, and not one that anyone other than the network operator should ever have access to.

So that's purely on the telco side.

On the radio network side, things are a little more complex. The way GSM works is that there are a few hundred radio channels, each 200 kHz wide, and they have numbers. There are a few control channels which a BTS puts out control messages. Each channel can support up to eight active calls, which would give you a total capacity of maybe a thousand users. This is obviously unacceptable for a national network so the way the system works is that the frequencies are reused.

An individual BTS uses channels a, b, c, d, e, f, then its neighbour is set up to use channels g, h, i, j, k, l, then one neighbour over from that, it reuses a, b, c, d, e, f. In urban environments where there are a lot of barriers to microwaves, they can reuse frequencies even very close together. Which is important, because the capacity of the network is directly proportional to the density of frequency reuse.

The frequency control and planning of such a network is extremely complex and difficult to get right because no two neighbours can reuse the same frequencies, and the terrain has a large impact on which frequencies are usable. So if the site owner was allowed to modify the configuration of the BTS they could potentially take down the entire network or at least make the network manager's job impossible.

http://en.wikipedia.org/wiki/Frequency_reuse#Frequency_reuse (some information on how it works in common technology here)

So...

Say there's an earthquake. Everyone picks up their cellphone and tries to call home. The first thing that happens is that your phone signals that it has a control message to send to the BTS. The BTS then sends a control message saying "phone 223949234 send your control message on slot 3 of channel 156." Your phone then sends a control message saying "I want to call +14152038512, and this is a hash of my credentials from the sim."

The BTS talks to its partner on the other end of the backhaul network and when it gets a connection, it sends back a control message to your phone saying "your originating call is available on channel 234 slot 6 and you should talk on slot 7."

What's important is that this whole process is coordinated across the airside network. If everyone tries to seize a channel at the same time, the cell's resources will be exhausted and it'll start saying "no," or alternatively, in some advanced networks it will try to hand the terminal off to a neighbour. UMTS and CDMA can do that; GSM can't. Normally, in a GSM network the BTSes are controlled in concert by a BSC, which is very firmly planted in AT&T's network.

a. Can wireless carriers implement a general service interruption, but still ensure that the public can make wireless 911 calls? Would a service disruption that permits wireless 911 calls, but otherwise prohibits voice, text, and data communications, achieve the same purpose as a blanket interruption? Would it pose any unique risks to persons with disabilities?

This is a really bad idea because it basically opens the door to allowing governmental entities a justification for creating BART-styled shutoffs – with the caveat that “customers will be safe” because they’ll still have access to 911, and / or to CMAS, or…. You get the picture. Also, please read my answer in 2(b) regarding the problem with blanket approvals (in a nutshell: very, very bad). Anything like what you are describing in this question is basically screaming out for a lawsuit, and as soon as you do it people will jump from expanding Line on their Androids, which is now at something like 30 million users, to installing mesh apps such as Serval on their phones and computers so that when you turn off our cell systems, we’ll just keep communicating and sending data.

b. Can wireless carriers implement a service interruption while ensuring that authorized parties would have uninterrupted access to wireless priority service (WPS)?

No. You may think so, but I don’t.

c. Can wireless carriers implement a service interruption and still provide targeted alerts via the Personal Localized Alerting Network (PLAN) to the public in the affected area?

See my answer to 4(a) above.

d. What are the costs and benefits of a service interruption where one or more of wireless 911, WPS, or PLAN are also disrupted?

Think of it as a loss of a cell site for every place that is no longer transmitting or receiving the desired information. See also http://www.ece.cmu.edu/~peha/paying_carriers_for_public_safety_use.pdf

e. What are the different methods for interrupting wireless service? How do circumstances affect the availability of these methods?
N/A – No comment

f. How do the effects differ among methods of interruption? Do some methods target a narrower geographic area?

N/A – No comment

g. What methods of interrupting service would lead to the most rapid restoration of service?

N/A – No comment

5. Authority to interrupt service. Which public institutions, agencies, or officials have or should have the authority to request an of interruption wireless service? What process should officials with such authority use to effectuate an interruption?
a. What processes could ensure that only an appropriate official makes the decision to request an interruption of wireless service? How would such an official be contacted in an emergency situation where time is of the essence?

The Communications Act provides instructions for the case in which this is to occur. It states in the Communications Act of 1934, "Upon proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President, if he deems it necessary in the interest of national security or defense, may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States as prescribed by the Commission, and may cause the closing of any station for radio communication, or any device capable of emitting electromagnetic radiations between 10 kilocycles and 100,000 megacycles, which is suitable for use as a navigational aid beyond five miles, and the removal therefrom of its apparatus and equipment, or he may authorize the use or control of any such station or device and/or its apparatus and equipment, by any department of the Government under such regulations as he may prescribe upon just compensation to the owners. The authority granted to the President, under this subsection, to cause the closing of any station or device and the removal therefrom of its apparatus and equipment, or to authorize the use or control of any station or device and/or its apparatus and equipment, may be exercised in the Canal Zone." Subsequent sections of the Act provide for review and challenge in the courts of any Presidential decision.

Contacting the President would likely occur through the internet and phones, but in such an event, for obvious reasons, it is possible the President would not be easily contacted by the public. Any mechanism that the public would find to contact the President if a decision were made by the President to shut down specific stations or devices would likely become overwhelmed by traffic from people commenting on the matter, even if a President had not concurrently shut down mechanisms enabling public contact with government. It is not advisable for a President to engage in a decision to deny the public access to stations or devices (which are part of what make up networks which many people rely upon) under any circumstances other than the sort mentioned in my answer at 2(b).

b. What institutions or officials should be able to review the decision to interrupt wireless service? What process considerations or safeguards should be implemented? How can timeliness of such review be ensured?

Focusing again on some of the proposed possibilities described in my answer to question 2(b) above, which was concerned with the possibility of intersection of nuclear device(s) with a cellular signal or signal(s) in some combination: J-3 (Operations) Directorate of the Joint Staff at the National Military Command Center (NMCC) and officials from the Office of the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Programs / Nuclear Matters should be advised in addition to the Federal Emergency Communications Coordinator, the Secretary of Defense and the President. According to the Communications Act, it is

the decision of the President to decide whether or not wireless service would be interrupted in such circumstances. Some information also can be determined via review of the policy of the of the Office of the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Defense Programs / Nuclear Matters (from NARP Internet Supplement, DoD 3150.8-M (4/27/2009)): "Fast, reliable, and accurate communications are essential for nuclear weapon accident or incident response operations. Moreover, securing adequate internal communications to support activities at the accident scene is a time sensitive operation. Equally critical to effective C2 is the timely establishment of external communications to higher levels, particularly in the Washington, D.C. area. The communications officers of the DoD IC must act immediately to ensure that appropriate communications equipment is identified and requested early in response operations. Information must be accessible. In general, the value of information increases with the number of users."
Some of the specific requirements of for this particular situation from the Office of the Assistant are: "Wireless Communications. Provide secure wireless nets such as UHF/VHF nets for command, weapons recovery operations, radiological operations, security, and public affairs.
Establish and assign radio call signs.
Establish a local computer network or access to a local computer network. If possible, establish virtual C2 requiring password access. The computer network should be
protected by an appropriate firewall and be able to access the Internet, accommodate e-mail, and ease document processing storage and recovery. Additionally, computer assets must be robust enough to securely maintain the potentially large amount of records which will be generated during all phases of the response operation. (...)
Internet access. The requirement to send and receive large data size documents and images between command authorities is probable. Therefore, Internet access should be as robust as practical. The communications officer should strive to provide bandwidth at 128Kbps or higher. SECRET Internet Protocol Router Network (SIPRNET) access is always desirable. If SIPRNET is available, the DOD IC and staff should consider the regular use of the SIPRNET chat room feature for keeping all concerned parties updated on the nuclear weapon accident response operation." (...)
"the Federal Emergency Communications Coordinator (FECC) (...) is the lead person on ESF#2. The FECC is the single Federal point of contact in the accident or incident area to coordinate the Federal telecommunications requirements and industry's response."
(...) "The local telephone company, State and/or local officials, or civilian authorities may provide information on the communication infrastructure near the accident or incident scene and the capabilities for long haul and local communications; this information is particularly important if the accident or incident damaged or destroyed portions of the communication infrastructure. Additionally, cell phone capabilities may be severely limited in a large scale accident due to over usage. Once existing capabilities are determined, the communications officer should use these resources with deployed assets to establish an effective communications network."
The following section of the document is also worth quoting here and commenting on: "In remote or sparsely populated areas, the initial communication capability may consist of only hand-held, short-range VHF/FM radios, portable HF radios, cellular telephones, or wire (field phones). Conversely, if an accident or incident occurs close to a populated area, a coin-operated telephone, cellular telephones, or even a business or private telephone may be available immediately for emergency use. In either case, additional leased communications, such as Wide Area Telephone Service (WATS), may be obtained to supplement available communications. Because more time is required to provide leased assets to remote areas, the requirements must be identified and requested at the earliest possible time. Follow-on deployment of mobile communications provides the response force with additional local telephone and radio, as well as long haul secure voice and record capabilities."

(The comment I have on this particular paragraph above is that while it does make mention of the possibility of use of cellular telephones in populated areas, it does not make reference to supportive software such as mesh network systems for Android phones. This was written in 2005 and so, some of the software that is becoming more common today, such as the Serval Project (mesh network embedded in cellular telephones), did not exist at the time the policy was written.)

The above quoted text is a small portion (relevant to this proceeding) of the recommendations from a paper on nuclear weapon accident or indicent from the Office of the Assistant to the Secretary of Defense at:
http://acq.osd.mil/ncbdp/narp/Functional_Areas/Communications.htm as of 4/17/12.
(On 4/17/12 the above information was accessed at the above link (where it was publicly posted in html format without any limitations or unique classifications that would restrict public viewing or quotation with attribution to the source.) By 4/19/12, however, the above information and link was no longer accessible online and was apparently online available via accessing a cached copy of the information.)
Google's cached copy of this as of April 19, 2012 is
at https://webcache.googleusercontent.com/search?q=cache:http://acq.osd.mil/ncbdp/narp/Functional_Areas/Communications.htm
Both of the above links provided the same information, which was the Communications section of the NARP Internet Supplement, DoD 3150.8-M (4/27/2009).
An alternate public source to information similar to that quoted above, which is available online without any limitations or unique classifications that would restrict public viewing or quotation with attribution to the source, was available as of April 19 and April 20, 2012 at: page 175 of http://www.dtic.mil/whs/directives/corres/pdf/315008m.pdf (DoD 3150.8-M, Feburary 22, 2005: Communications) in which, strangely, references to the use of cellular telephones for emergency use were not included. A updated

source for this information may have been made available after May of 2009, when a new draft document was under review, but it is unavailable at the time of filing of this comment. It is thought that the cached copy and content shown above cited from and accessed on 4/17/12 at http://acq.osd.mil/ncbdp/narp/Functional_Areas/Communications.htm and accessed on 4/19/12 at https://webcache.googleusercontent.com/search?q=cache:http://acq.osd.mil/ncbdp/narp/Functional_Areas/Communications.htm, which includes references to cellular telephones for emergency use, is the most up-to-date content readily available on the subject of how U.S. defense organizations should approach telecommunications issues in the context of a nuclear incident.
The Hon. Andrew C. Weber is presently the principal advisor to the Secretary of Defense, the Deputy Secretary of Defense, and the Under Secretary of Defense for Acquisition, Technology and Logistics for matters concerning nuclear, chemical, and biological defense programs, and is the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs.
(Refer to http://www.defense.gov/bios/biographydetail.aspx?biographyid=232)

c. What obligations do or should wireless carriers have to comply with a request by a government official to interrupt wireless service?

If wireless carriers have received an order from a court, or a transmittal from the Federal Communications Commission, for example, showing evidence of an approval of a request for modification or discontinuance of service, then a wireless carrier may feel quite compelled to "interrupt" wireless service. However, the carrier is obligated to comply with the Communications Act and as such, should not automatically comply with a request by a governmental official merely because the request exists. Instead, the carrier should examine from whom the request comes (if it is coming from a local government official, for example, there is no authority and thus the carrier can safely ignore the pleas and whinings of the local government entity that wishes to turn off cellular and / or wireless service)

d. What steps should be taken to ensure a timely return to full wireless service in the affected area? What institutions or officials should have authority to request a return to full wireless service in the affected area?

Don't turn it off in the first place. But if you make that mistake, turn it back on right away.

e. What procedures should there be to review an interruption after it has occurred?

The nature of this question is problematic. No "interruption" should occur without there first being an application approved consistent with the Communications Act. See my answer to question 2(b) above. See also my answer to 5(a).
Also, please note that under the Communications Act, it states that with respect to "TREATMENT OF PUBLISHER OR SPEAKER.--No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Thus there is no justification for interruption of service by anyone -- regardless of whether their status is as a common carrier with respect to some of the services they are engaged in providing, with repect to all services, or some other status. Any governmental actor engaged in the provision (at any level, even if seperated from direct providing) of cellular service and / or wireless internet, and / or enhanced services of any kind, will still have violated the Communications Act if the governmental actor has taken part in, been party to, or facilitated an "interruption" (modification, discontinuance, etc.) without first having gotten permission from the Federal Communications Commission with review and any necessary decision from the relevant state commission of appropriate jurisdiction, or a court of law with appropriate jurisdiction. Please see further documents and details within this proceeding at:
http://apps.fcc.gov/ecfs/comment/view?id=6017027782

6. Legal constraints on interrupting wireless service. Many laws—local, state, federal, constitutional—could prohibit or constrain the ability to interrupt wireless service. The legality of an interruption could depend upon particular circumstances, such as the reason for the interruption, its duration, its geographic scope, or how the interruption is accomplished. What are the laws or regulations that affect the legality of an interruption, and what are the circumstances that are likely to render an interruption permissible or impermissible?

Some US code pertaining to this question can be found here - http://law.onecle.com/uscode/47/index.html

Taken from http://www.fcc.gov/encyclopedia/jammer-enforcement, some of the law applicable to cell phone jammers may apply here, for example, Sections 333, 503:

- *The Communications Act of 1934*
  - Section 333 - prohibits willful or malicious interference with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government (47 U.S.C. § 333)***

- Section 503 - allows the FCC to impose forfeitures for willful or repeated violations of the Communications Act, the Commission's rules, regulations, or related orders, as well as for violations of the terms and conditions of any license, certificate, or other Commission authorization, among other things.

- *The Criminal Code* (Enforced by the Department of Justice)
  - Title 18, Section 1362 - prohibits willful or malicious interference to US government communications; subjects the operator to possible fines, imprisonment, or both (18 U.S.C. § 1362)
  - Title 18, Section 1367(a) - prohibits intentional or malicious interference to satellite communications; subjects the operator to possible fines, imprisonment, or both (18 U.S.C. § 1367(a))

Please see also:
The Public Knowledge Petiton for Declaratory Ruling
http://www.publicknowledge.org/files/docs/publicinterestpetitionFCCBART.pdf
An Ex Parte Presentation of Colin G. Gallagher (filed via ECFS in proceeding 12-52)
http://apps.fcc.gov/ecfs/comment/view?id=6017027782

a. What sources of legal authority does the Commission have regarding shutdowns of wireless service? What discretion does the Commission have to approve or disapprove shutdowns?

While the legal ramifications of a Commission approval of a shutdown are presently unclear due to various competing proposed laws at the state, federal, and even international level having to do with this sort of issue, at present the Commission rules for discontinuance, reduction, or impairment of service can be found on its website:
http://transition.fcc.gov/wcb/cpd/other_adjud/business214.html

b. Are there circumstances under which a government entity could be construed to have common carrier obligations under the Communications Act due to its relationship with or control over wireless service?

Please see the complaint by Colin G. Gallagher in this proceeding (12-52), received via ECFS on 4/09/2012 and posted 4/10/2012. This complaint describes the specific circumstances under which a government entity can be construed to have common carrier obligations under the Communications Act due to its relationship with or control over wireless service. The complaint as a filing in this proceeding can be seen directly at: http://apps.fcc.gov/ecfs/comment/view?id=6017029061 Please also see e-CFR data at 47 CFR §22.99 describing a Telecommunications common carrier, see also the meaning of the term "public mobile services" in the Communications Act of 1934, and finally see HR Conf. Rep. No. 1918, 73d Cong., 2d Sess. 46 (1934). While the "for hire" caveat may be debated, it is well known that in the context of any free wireless service to the public, for example, where free wi-fi internet is provided as part of a service available while on a San Francisco Bay Area Rapid Transit District train or an Amtrak train, as examples, these services are only available where a customer has first paid for access to the area of service via a fare, thus arguably bringing common carriage obligations to such a governmental actor providing enhanced services. Additionally, distinct from the Communications Act, in CALEA, 18 USC 2510, "a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title" can be considered to be a telecommunications carrier (for CALEA). (See also: In re Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), Docket No. 20828, Final Decision, 77 FCC2d 384 (May 2, 1980) (*Computer II* Final Decision).) The various NARUC cases also show, collectively, that it is possible for a governmental entity, including a railroad, to be a common carrier, within the context of both the Communications Act and case law, with regard to some of its activities but not others (with respect to "a portion of its service only") when governmental actors and their agents are engaged in the provision of cellular and / or wireless internet or various enhanced services, in such a way that renders the governmental actors as common carriers with respect to certain cellular and / or internet services that they are engaged at some level in the provision of to the public (even if the governmental actors are not directly providing the service). Within the context of
47 USC § 153(51), it is felt by this commenter that the Commission should treat and interpret governmental actors providing cellular and / or internet service, whether or not for hire, as a “telecommunications carrier” (mean(ing)) "any provider of telecommunications services," but should not treat the governmental actor(s) as "aggregators of telecommunications services." (In support of this assertion, see also §332(c)(1)(A) of the Communications Act of 1934 [47 U.S.C. 332], having to do with common carrier issues relating to "person(s) engaged in the provision of a service that is a commercial mobile service.")
Please also refer to Ex Parte Presentation of Colin G. Gallagher received 3/30/2012 and posted 4/02/2012 available in this proceeding (12-52) at http://apps.fcc.gov/ecfs/comment/view?id=6017027782
Again, looking at all of this together, this all emphasizes the necessity for the Commission to interpret governmental entities as telecommunications common carrier(s) under the Communications Act, as telecommunications carriers within the context of CALEA,

and as telecommunications carriers within the context of 47 USC § 153(51). It is the sense of the commenter that taken together, these above comments demonstrate the common carrier obligations of governmental entities such as the San Francisco Bay Area Rapid Transit District, or any local, regional, state governments, or federal agencies, which provide cell and / or wireless services to the general public. Finally, it is strongly felt that forbearance from applying such provision or regulation (including the Communications Act of 1934, CALEA, Telecommunications Act of 1996, and similar laws), if requested by governmental entities / actors (and/or by corporate entitites and any third party providers that are contracted by governmental actors to provide cellular and / or wireless internet services to the general public on behalf of the governmental actors) is not consistent with the public interest. Forbearance is inappropriate, wrong, and not in the public interest, and the same goes for any other means of petitioning for exemption from any regulation which allows for Federal Communication Commission control, oversight, and ability to penalize any organization or entity which attempts to shut down networks used by the general public. Federal Communication Commission regulation, rulemaking, oversight, and ability to penalize can help ensure that San Francisco Bay Area Rapid Transit District styled shutdowns will not be repeated.

c. What authority does the Commission have to preempt laws and regulations permitting or prohibiting interruption of wireless service? How should the Commission exercise any such authority?

Within the context of this proceeding, the Commission has opted to open the proceeding (12-52) as a permit-but-disclose proceeding, thus the public serves a role in facilitating the initiation of the Commission's use of its authority for pre-emption in the context of this proceeding (12-52) to the extent that the general public and the Commission use the rules for this purpose. This proceeding is a permit-but-disclose proceeding. According to the rules for this proceeding as established by the notice, 47 C.F.R. §§ 1.1200(a), 1.1206. et seq., which can be found at http://www.fcc.gov/encyclopedia/ex-parte-rules-2011, at Note 1 to paragraph (a) (of §1.1206(a)): "In the case of petitions for declaratory ruling that seek Commission preemption of state or local regulatory authority, the petitioner must serve the original petition on any state or local government, the actions of which are specifically cited as a basis for requesting preemption. Service should be made on those bodies within the state or local governments that are legally authorized to accept service of legal documents in a civil context. Such pleadings that are not served will be dismissed without consideration as a defective pleading and treated as a violation of the ex parte rules unless the Commission determines that the matter should be entertained by making it part of the record under § 1.1212(d) of this section and the parties are so informed." Service of process rules are found at 47 CFR §1.47 which can be found at http://www.law.cornell.edu/cfr/text/47/1.47 and for such petitions for declaratory ruling which are formal complaint proceedings against common carriers, require the format of general pleading requirements at 47 CFR §1.720 which can be found at http://www.law.cornell.edu/cfr/text/47/1.720
It is worth noting here (again) that any attempted forbearance from applying provision(s) or regulation is not consistent with the public interest.

In order that the Commission may exercise preemption of a state or local regulatory authority (such as the San Francisco Bay Area Rapid Transit District) - in particular, in order that the Commission may do so within the proceeding 12-52 - all that is necessary is for someone to have found an agent to perform service of process for them, to serve the authority (government actor) with a cover and petition for declaratory ruling, and then to file (via the ECFS system) a copy of the relevant documents once served. (Please see also Title II - §208 of the Communications Act of 1934 [47 U.S.C. 208] and [47 U.S.C. 332]). Thus, in the context of this proceeding (12-52), please refer (as an example) to the Ex Parte Presentation of Colin G. Gallagher, received in the ECFS 3/30/2012 and posted 4/02/2012, which contains within its pages proof of service of process on the San Francisco Bay Area Rapid Transit District and a copy of a Petition for Declaratory Ruling, which can be viewed at http://apps.fcc.gov/ecfs/comment/view?id=6017027782
The Petition for Declaratory Ruling was submitted subject to Federal Communications Commission Rule 1.2, or 47 CFR §1.2. According to this section, "The Commission may, in accordance with section 5(d) of the Administrative Procedure Act, on motion or on its own motion issue a declaratory ruling terminating a controversy or removing uncertainty." Clearly, the Commission should issue a declaratory ruling in the matter of the San Francisco Bay Area Rapid Transit District and the matter of the events of August 11, 2011, but also in the broader matter of creating a ruling that will prevent such events from happening again. The Petition was received by the Federal Communications Commission on 9/09/2011 (see last page of document, USPS confirmation page). It has not been withdrawn, and when the Commission opened this proceeding (12-52) as a permit-but-disclose proceeding, an electronic copy of it was served on the San Francisco Bay Area Rapid Transit District, and it was filed into the record for this proceeding, in accordance with the rules for this proceeding as established by the notice, 47 C.F.R. §§ 1.1200(a), 1.1206. et seq. and 47 CFR §1.47.

d. What protections do the First Amendment or due process rights provide for users of wireless service? Under what circumstances could an interruption of wireless service violate the First Amendment or due process rights of wireless users? Are there other constitutional protections that should be considered?

The righs for users of wireless service are extensive. See, for example:
120 P.2d 946 (Cal. App. 1942).
81 So. 2d 254 (1955)
Shillitani v. Valentine, 184 Misc. 77, 81 (N.Y. Sup. Ct. 1945).
Nadel v. New York Tel. Co., 9 Misc. 2d 514, 516 (N.Y. Sup. Ct. 1957)
Shillitani, 184 Misc. at 80 (N.Y. Sup. Ct. 1945)
220 F. Supp. 621 (N.D. Ill. 1963)

e. What protections do the First Amendment, due process, or other constitutional rights afford wireless carriers? Under what circumstances could a forced interruption of wireless service violate the First Amendment, due process, or other constitutional rights of wireless carriers?

In every circumstance except where there is a routine, brief (and authorized) interruption for maintenance reasons, you will find First Amendment, due process, and other constitutional rights being violated by anyone who opts to "interrupt" a wireless service.

f. What provisions of Title II of the Communications Act prohibit or circumscribe an interruption of wireless service, and under what circumstances? To what extent do sections 202, 214, 302a, 333, or other sections of the Communications Act circumscribe the ability of government actors to interrupt wireless service?

The following is a quotation from the Public Knowledge Petition for Declaratory Ruling. It is unknown to this commenter at the time of filing this comment whether or not Public Knowledge has pursued its Declaratory Ruling or withdrawn it in light of this proceeding. However, the argument presented in Public Knowledge's Petition is legitimate.

"II. Carriers May Not Disconnect Service Without Authorization
A. Interruption of CMRS Conflicts with Section 214(a)(3).
It is possible that BART's contractual arrangements with CMRS carriers, or its own
actions, would provide sufficient basis for the Commission to determine that BART is a CMRS carrier or an "agent" of CMRS carrier. Should BART be found to have operated the underground network as a carrier, its deliberate interruption of service conflicts with common carrier duties under Sections 214(a)(3) and 202. CMRS is a Title II telecommunications service under Section 332(c), and providers of Title II service are bound by the requirements to provide service and refrain from unjust or unreasonable discrimination in practices. The Commission must clarify that disruption of the CMRS networks is therefore subject to the same restrictions under Title II as disruption of the wireline telephone network.
Section 214(a)(3) states: No carrier shall discontinue, reduce, or impair service to a community, or part of a community, unless and until there shall first have been obtained from the Commission a certificate that neither the present nor future public convenience and necessity will be adversely affected thereby..."
"BART's turning off of its underground network clearly discontinued and impaired service to its customers. In the absence of authorization from the Commission, BART's discontinuation of service should be ruled a violation of Section 214. Furthermore, Section 202 prohibits "unjust and unreasonable discrimination in...practices...facilities, or services...directly or indirectly, by any means or device..." (16) / Footnote 16:
47 U.S.C. § 202(a)."
(from http://www.publicknowledge.org/files/docs/publicinterestpetitionFCCBART.pdf)

The FCC has clear jurisdiction over devices which interfere with radio reception. (See 47 U.S.C. 302a). Local and state governments may make rules over the use of citizen's band radio equipment (See 47 U.S.C. 302f) except that "A station that is licensed by the Commission pursuant to section 301 of this title in any radio service for the operation at issue shall not be subject to action by a State or local government under this subsection." "The Commission shall, to the extent practicable, provide technical guidance to State and local governments regarding the detection and determination of violations of the regulations specified in paragraph (1)."

http://law.onecle.com/uscode/47/302a.html

g. What state laws prohibit or circumscribe an interruption of wireless service? What authorities do state public utility commissions have to prohibit or circumscribe an interruption of wireless service? Are there circumstances in which approval of a state public utilities commission is necessary before ordering a shutdown?

It is hoped that the California Public Utilities Commission, Communications / Telecommunications Division, will provide comment to answer this question.

h. To what extent does a public agency's contractual or practical control over wireless service equipment affect the analysis of whether a public agency has the legal authority to interrupt wireless service?

Please see my answers to 1a, 2a, 6b, 6c.

i. What is the scope of the Commission's discretion to set policies that affect a public agency's legal authority to interrupt wireless service? To the extent the Commission has not exercised this discretion, should it do so, and in what ways?

Please refer to page 12 and 13 of http://www.publicknowledge.org/files/docs/publicinterestpetitionFCCBART.pdf and also refer to my answers to question 6(c) above.
Finally, please consider the following: In the U.S. Supreme Court it was stated that, "Congress meant to confer "broad authority" on the Commission (H. R. Rep. No. 1850, 73d Cong., 2d Sess., 1 (1934)), so as "to maintain, through appropriate administrative control, a grip on the dynamic aspects of radio transmission." (FCC v. Pottsville Broadcasting Co., 309 U.S. 134, 138 (1940)). To that end, Congress subjected to regulation "all interstate and foreign communication by wire or radio." (U.S. Supreme Court, FCC vs. Midwest Video Corp., No. 77-1575 (1979))